UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

FERROVIAL CONSTRUCTION US CORP., NORTH PERIMETER CONTRACTORS, LLC, FERROVIAL CONSTRUCTION EAST, LLC and ALAMO NEX CONSTRUCTION, LLC, Plaintiffs, VERSUS JESUS GONZALEZ FERNANDEZ, DOMINGO RODRIGUEZ TORREGROSA, MICHAEL VALDES, JOSE LUIS BELTRAN, MARIA BREGEL SERNA, and ACCIONA CONSTRUCTION USA CORP., Defendants.	CIVIL ACTION NO. 1:25-CV-0804-LMM

MEMORANDUM IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION AND TO SET EVIDENTIARY HEARING

Plaintiffs, Ferrovial Construction US Corp. ("FCUS"), North Perimeter Contractors, LLC ("NPC"), Ferrovial Construction East, LLC ("FC East"), and Alamo NEX Construction, LLC ("ANC") (collectively, "Plaintiffs") file this memorandum in support of their *Motion for Preliminary Injunction* (the "PI Motion").

1. Plaintiffs are part of a corporate family of businesses whose ultimate parent is Ferrovial SE ("Ferrovial"), which is internationally recognized for its unique ability to design and develop large-scale transportation infrastructure projects. FCUS is focused on design-build projects throughout North America. FC

East, a FCUS subsidiary, is an entity responsible for operations in the eastern region of the United States. NPC, which is a subsidiary of FC East and an indirect FCUS subsidiary, is a special purpose entity formed to complete the Transform 285/400 project at the interchange of I-285 and SR400 (the "285/400 Project"). ANC is a special purpose entity formed to complete the I-35 NEX Central project in Bexar and Guadalupe Counties, Texas, under contract to the Texas Department of Transportation. Like NPC, ANC is an indirect subsidiary of FCUS.

2. The individually-named defendants — Jesus Gonzalez Fernandez ("Gonzalez"), Domingo Rodriguez Torregrosa ("Rodriguez"), Michael Valdes ("Valdes"), Jose Luis Beltran Simal ("Beltran"), Maria Bregel Serna ("Bregel") (collectively, the "Individual Defendants")) — were each long-time employees within the Ferrovial corporate family, but they are now working to launch new operations within the Greater Atlanta area and Southeast region for a competitor, Defendant Acciona Construction USA Corp. ("Acciona") (Acciona and the Individual Defendants are collectively, the "Defendants").

3. Plaintiffs filed the PI Motion to enjoin Defendants from disclosing, using, and continuing to retain Plaintiffs' trade secrets and, as detailed below, Plaintiffs can show — whether at an evidentiary hearing or based on the pleadings — that they are entitled to the requested preliminary injunction to preserve the status quo and prevent irreparable harm.

SUMMARY OF ARGUMENT

4. By the end of 2024, it had become apparent to Plaintiffs that something was amiss. Three high-ranking, long-term, management-level employees (Rodriguez, Gonzalez, and Valdes) abruptly resigned. They suggested that they were leaving to help a competitor — Acciona — establish a new presence within in the Greater Atlanta area and the Southeast region.

5. Around this same time, Plaintiffs' internal cybersecurity team alerted Plaintiffs to potentially suspicious computing activity on Gonzalez's computer. Before his last day of employment, Gonzalez had transferred a large amount of commercially-sensitive data to external storage devices. This prompted an immediate internal investigation, with Plaintiffs engaging not only outside legal counsel but also computer forensic experts. The investigation — which included interviews of Gonzalez — made clear that litigation was necessary. Gonzalez not only intentionally retained possession of Plaintiffs' most valuable information, but he also was actively trying to obfuscate and conceal this misappropriation.

6. Plaintiffs hoped that their exposure would be limited to Gonzalez's misconduct and that they could reach a resolution with him that avoided the need for protracted litigation. Those hopes were ultimately dashed. While a potential resolution was being explored, Plaintiffs continued their internal investigation, which uncovered a wide-ranging scheme. Gonzalez was not the only employee

engaged in computing misconduct; so too were Rodriguez (a Managing Director) and Valdes (a Human Resources Manager). Rodriguez used external storage devices to misappropriate a large volume of Plaintiffs' most sensitive information — and he was even surreptitiously attending meetings with Acciona while he was engaged in this computing misconduct. Valdes used external storage devices to misappropriate highly sensitive information relating to wages and employee information that would make it substantially easier to recruit talent away to Acciona. Valdes too took significant efforts to hide this misappropriation, including lying to counsel. These three individuals — who worked for years together within the Ferrovial corporate family — did not coincidentally resign at the same time, join their competitor Acciona, and each happen to retain external storage devices with misappropriated trade secrets. These actions were part of a concerted plan — or, to put it differently, a civil conspiracy — to steal trade secrets to improperly benefit Acciona.

7. But just as Plaintiffs were drawing these conclusions, Plaintiffs learned that this concerted plan included others. Plaintiffs received notice that Beltran and Bregel — who are married and were long-term employees within Ferrovial's corporate family — were leaving ANC in Texas to also help launch Acciona's operation in the Greater Atlanta area and the Southeast region. Between the two of them, they used external storage devices to misappropriate over three hundred thousand documents before joining Acciona.

8. Ultimately, Plaintiffs' investigation made clear that its competitor, Acciona, is amassing a growing team of former Ferrovial personnel, armed with an arsenal of Plaintiffs' most commercially-sensitive documents. The need for a preliminary injunction is dire, and Plaintiffs can offer evidence to satisfy the requirements for issuing the requested injunctive relief. ***First***, Plaintiffs can establish that they are likely to succeed on the merits of their trade secret claims, as the Defendants have misappropriated information that Plaintiffs' take reasonable measure to keep confidential and that has economic value from being kept confidential.[1] ***Second***, Plaintiffs will suffer irreparable harm in the absence of preliminary relief. ***Third***, the balance of equities tips in favor of granting the preliminary injunction, as Plaintiffs are merely seeking an order that prevents Defendants from engaging in unlawful and unfair competition and requires the preservation and return of stolen property. ***Fourth***, the requested injunction is in the public interest because it bolsters fair competition in the marketplace.

[1] Plaintiffs have claims under Defend Trade Secrets Act, 18 U.S.C. § 1125 *et seq.* ("DTSA"), the Georgia Trade Secrets Act, O.C.G.A. § 10-1-760 *et seq.* ("GTSA") and the Texas Uniform Trade Secrets Act, TEX. CIV. PRAC. & REM. C. § 134A.001 *et seq.* ("TUTSA").

FACTUAL BACKGROUND

Plaintiffs' Business and Their Trade Secrets

9. FCUS, as part of the Ferrovial family of corporate entities, operates as a leading contractor within the transport infrastructure industry by providing civil infrastructure solutions through its unique ability to leverage the engineering and construction expertise it has fostered across its family of businesses and over many decades. FCUS performs design and construction of sustainable, innovative, and efficient infrastructure for governmental owners and for Ferrovial affiliates, which develop and operate such projects across the United States. The Greater Atlanta area is a key market for Ferrovial, and the prospective infrastructure projects within it are strategic targets. *See* R. Doc. 9, *Verified First Amended Complaint* ("FAC"), at ¶ 29. Ferrovial operates through a family of corporate entities, many of which have specific responsibilities based on the individual needs of large-scale infrastructure projects. One such corporate entity is FC East, which is focused on the East Coast operations of Ferrovial's construction division. Other such corporate entities include NPC, which is focused on the completion of an existing large-scale infrastructure project within the Atlanta-metro area, and ANC, which is focused on the completion of the I-35 NEX Central Project in and around San Antonio, Texas. (FAC ¶ 30).

10. A substantial part of Ferrovial's competitive position lies in its confidential business information. This information is one of the Ferrovial corporate

family's greatest assets. Accordingly, Ferrovial takes substantial care to keep this information out of its competitors' hands. (FAC ¶ 31). To protect this information, Plaintiffs require employees to agree to various policies and procedures designed to protect the information's confidentiality. For instance, employees must agree to be bound by a "Corporate Code of Ethics" that states: "Ferrovial's proprietary and confidential information is one of its greatest assets," which includes "[t]echnical information, designs, process data, pricing information, strategic plans, know-how, software and technology." It further states that employees "should never use Ferrovial's confidential information – or that of third parties – outside the scope of the professional context in which it was originally obtained" and that "Ferrovial's property should never be used for offensive or illegal purposes, conducting personal or other business, or to further the activities of a competitor."[2] (FAC ¶ 32).

11. Employees also agree to be bound by the "Procedure for the Use of Technological Resources," which serves the purpose of "safeguarding the integrity, confidentiality, and availability of Ferrovial's information;[3] and the "Competition Policy," which specifically prohibits the exchange of confidential business

[2] A true and correct copy of the "Corporate Code of Ethics" is attached as **Exhibit 1**.

[3] A true and correct copy of the "Procedure for the Use of Technological Resources" is attached as **Exhibit 2**.

information among competitors.[4] In fact, just to accomplish the everyday task of simply logging into their computer, each of the Individual Defendants (like all employees with access to Ferrovial's computing network) were required to acknowledge and agree that their access was granted for the limited purpose of performing work for Ferrovial and was given subject to compliance with the Procedure for the Use of Technological Resources. (FAC ¶ 33). The Individual Defendants were bound by these policies during their employment with Ferrovial, up to and including the dates on which each of them saw fit to expropriate Ferrovial's trade secrets and other sensitive / proprietary information. (FAC ¶ 34).

12. Plaintiffs protect their confidential information on password-protected internal computer servers that can only be accessed by select employees who have a valid reason to review or use the information. Many of Ferrovial's sensitive documents are protected further still, such that only certain management-level employees within Ferrovial have the ability to access or modify sensitive data points within the documents. Plaintiffs also train their employees, including all new hires, with access to confidential company documents that the documents are confidential and valuable to Plaintiffs and may not be disclosed to anyone outside of the Ferrovial family of businesses. And, like many businesses with valuable data to protect,

[4] A true and correct copy of the "Competition Policy" is attached as **Exhibit 3**.

Plaintiffs are able to monitor employees' computing activity and do so in order to safeguard their trade secrets. (FAC ¶ 35). Plaintiffs have instituted these measures because this information, in the hands of a competitor, can be used to compete unfairly and could cause irreparable harm. (FAC ¶ 36).

Investigative Stage One: Gonzalez

13. Gonzalez started working within the Ferrovial family of businesses seventeen years ago. During that time, Gonzalez was provided a company-issued computer as well as access to a password-protected network that contained various trade secrets relating to past, current, and prospective projects that he may need to perform his duties. (FAC ¶ 37). Most recently, Gonzalez was assigned by Ferrovial to perform design management services for NPC on the 285/400 Project and for FCUS in its pursuit of certain infrastructure projects within the Greater Atlanta area. (FAC ¶ 38).

14. However, during this time, there were other bids for prospective projects within the Greater Atlanta area that Gonzalez had no role in developing. Some examples were bids for the SR400 Express Lanes Project and "Sensitive Project No. 1."[5] (FAC ¶ 39). During the summer of 2024, NPC was focused on completing the 285/400 Project; but there were other infrastructure projects within

[5] To protect the commercially sensitive nature of this project, Plaintiffs have renamed it "Sensitive Project No. 1."

the Greater Atlanta area that came up for bid in this same timeframe: the West Interchange Project and the SR400 Express Lanes Project. (FAC ¶ 40).

15. Gonzalez was designated as the Proposal Design Manager on the West Interchange Project, and that bid was submitted on June 12, 2024. (FAC ¶ 41). Shortly before this bid submission, on May 7, 2024, the bid for the SR400 Express Lanes Project was submitted, but Gonzalez was not materially involved in developing the design for that bid. Rather, on that project, he participated in developing a design quality management plan and certain schedule items. (FAC ¶ 42). Both the West Interchange Project and the SR400 Express Lanes Project were subject to a competitive bid process. In fact, there were only two bidding consortiums on the SR400 Express Lanes Project. Ferrovial represented one; and Acciona was a member of the other competing team that also submitted a bid on the SR400 Express Lanes Project. (FAC ¶ 43).

16. From June 12, 2024, through August 14, 2024, while awaiting decisions on which bidding team would be awarded these two projects, various preparation meetings were convened to discuss plans if Ferrovial were successful in either or both bids. Gonzalez participated in these meetings. (FAC ¶ 44). But, on August 15, 2024, Plaintiffs learned that the SR400 Express Lanes Project was awarded to the competing team, of which Acciona is a member. (FAC ¶ 45). Shortly thereafter, attention shifted to Sensitive Project No. 1. Meetings began to be held about the

strategy for bidding this project, including the possibility of involving Gonzalez in the bidding process once he concluded certain matters associated with the ongoing 285/400 Project that NPC was working to complete. (FAC ¶ 46). From late August through November 13, 2024, Gonzalez participated in internal strategy meetings about Sensitive Project No. 1. He also participated in meetings on November 13-14, 2024 with strategic business partners who would be involved in the bidding process. (FAC ¶ 47).

17. Nevertheless, on November 19, 2024, Gonzalez unexpectedly gave notice of his resignation. He had accepted a position with Acciona, which had been awarded the SR400 Express Lanes Project over Ferrovial. But, at no point during the months-long series of internal and partner meetings prior to his resignation did Gonzalez ever disclose that he had been in talks with Acciona for potential employment. (FAC ¶ 48). Around the time of Gonzalez's resignation notice, Plaintiffs' internal cybersecurity team alerted Plaintiffs to potentially suspicious computing activity from Gonzalez's computer. Specifically, Plaintiffs' monitoring software indicated that there were mass transfers of documents from Plaintiffs' computing network to external storage devices plugged into Gonzalez's work-issued computer. (FAC ¶ 49-50).

18. Plaintiffs conducted an internal investigation to further examine this activity and discovered alarming facts. From late October 2024 through November

15, 2024 (*i.e.*, four days before his resignation notice), Gonzalez transferred nearly 100,000 documents from Plaintiffs' computing network to external storage devices, including confidential business information relating to projects and bids in which Gonzalez was not materially involved. (FAC ¶ 51). For instance, on October 26, 2024, Gonzalez started transferring over ***10,000 documents***, several of which related to the bid for the SR400 Express Lanes Project that Gonzalez did not materially work on. (FAC ¶ 52). The same type of misconduct occurred in the days leading up to his unexpected resignation notice:

- October 27, 2024: Gonzalez transferred over ***18,000 documents***;
- October 28, 2024: Gonzalez transferred over ***11,700 documents***;
- October 29, 2024: Gonzalez transferred over ***6,600 documents***;
- October 30, 2024: Gonzalez transferred over ***13,200 documents***;
- November 4, 2024: Gonzalez transferred over ***7,800 documents***;
- November 5, 2024: Gonzalez transferred over ***12,100 documents***;
- November 6, 2024: Gonzalez transferred over ***14,800 documents***;
- November 7, 2024: Gonzalez transferred over ***7,400 documents***;
- November 8, 2024: Gonzalez transferred over ***400 documents***, including a .pst file (containing numerous emails) and documents relating to the SR400 Express Lanes Project;
- November 11-12, 2014: Gonzalez transferred over ***50 documents***, some of which related to Sensitive Project No. 1 that Gonzalez was not yet materially involved in;

- November 13, 2024: Gonzalez transferred over ***600 documents***;
- November 14, 2024: Gonzalez transferred more business-related documents; and
- November 15, 2024: Gonzalez transferred several .pst files (full of numerous emails), as well as files related to the SR400 Express Lanes Project that Gonzalez was not materially involved in.

(FAC ¶ 53).

19. Plaintiffs' discovery of Gonzalez's misconduct led them to hire computer forensic experts, who have independently confirmed the significant exfiltration of data from Plaintiffs' computing network to external storage devices that were plugged into Gonzalez's work-issued computer. (FAC ¶ 54). In addition, the reports on Gonzalez's computing activity even showed that Gonzalez was attending meetings with Plaintiffs' competitor—Acciona—regarding the SR400 Express Lanes Project even before Gonzalez notified Plaintiffs that he was resigning to join Acciona. (FAC ¶ 55). Further, forensics on external storage devices that Gonzalez returned in response to the demand of Plaintiffs' counsel indicated more alarming facts. For instance, Plaintiffs' internal monitoring reports indicated that Gonzalez had transferred folders that contain sensitive information to an external storage device, including folders titled "4. Sensitive Project No. 2"[6] on 10/28/2024

[6] To protect the commercially sensitive nature of this project, Plaintiffs have renamed this folder "Sensitive Project No. 2."

at 2:38 PM; "21 DSA TEMPLATES on 10/30/2024 at 5:02 AM; "22. DOWNLOADS FERRO LAPTOP" on 10/30/2024 at 2:30 PM; "23 CONTRATOS INGENIERIAS" on 10/31/2024 at 3:05 PM; "Correo" on 11/7/2024 at 2:40 AM; "Jesus Correo" on 11/15/2024 at 12:14 PM; "13. Sensitive Project No. 1" on 11/12/2024 at 9:34 PM; and "22. DESKTOP FILES" on 11/04/2024 at 1:54:00 PM. However, when Gonzalez returned this external storage device, all of those folders had been removed, which strongly indicates that Gonzalez had plugged the device into some other computer (*i.e.*, not his Ferrovial work computer) to remove those folders from the external storage device. (FAC ¶ 56).

20. In addition to the obvious, this presents two potentially-serious problems. First, those folders remain unaccounted for. Second, another computing device has been used to access and manipulate the misappropriated information. Gonzalez has neither identified that device nor provided it for forensic examination. (FAC ¶ 57). Additionally, the forensics on Gonzalez's work computer also indicate that there are three unaccounted-for external storage devices that Gonzalez plugged into his work computer shortly before resigning. These include (i) a WD Easystore 2624, last connected on 8/1/24 and last disconnected on 8/2/24; (ii) a WD

MyPassport 25EA, last connected on 10/26/24 and last disconnected 10/28/24); and (iii) a Seagate BUP, last connected (and disconnected) on 11/15/24. (FAC ¶ 58).

Investigative Stage Two: Rodriguez and Valdes

21. After Plaintiffs filed their initial suit against Gonzalez (in this civil action), further evidence came to light, which inculpated other former, high-ranking employees that worked with Gonzalez and left with him to help lead Acciona and its efforts to expand its business. (FAC ¶ 59).

Managing Director Rodriguez

22. Like Gonzalez, Rodriguez had a long history of employment within the Ferrovial family of businesses. During his tenure of over two decades, he continued to ascend within the organization and was most recently promoted to Managing Director for the East Coast operations of Ferrovial's construction division that compromised major projects within Georgia, North Carolina, Tennessee, and Florida. (FAC ¶ 60). As Managing Director, Rodriguez was responsible for steering the East Coast business toward its strategic goals while overseeing daily operations. Rodriguez served as the primary representative in critical negotiations, stakeholder engagements, and major business decisions for the East Coast. Further, in this position, Rodriguez oversaw and supervised the work of Gonzalez and Valdes as well as other high-ranking employees, and he had access to some of Plaintiffs' most commercially sensitive information. (FAC ¶ 61).

23. Rodriguez also never disclosed while he was attending to internal and partner meetings regarding highly sensitive matters before his resignation that he had been in discussions with Acciona about potential employment. As with Gonzalez, the forensic evidence gathered during Plaintiffs' investigation revealed that Rodriguez also used external storage devices to misappropriate confidential information shortly before resigning to take an executive-level position at Acciona as "US Construction Director." (FAC ¶ 62). Specifically, on September 30, 2024, Rodriguez plugged in a "My Passport 260D" (serial number: WX62A44N277Y) to his work computer and transferred numerous folders and subfolders that housed over ***800 files***, including files that related to Sensitive Project No. 1, Sensitive Project No. 2 and Sensitive Project No. 3,[7] as well as documents relating to the 285/400 Project, SR400 Express Lanes Project, East Interchange Project, and various other projects within and outside the East Coast operations of Ferrovial's construction division. Further, on September 27, 2024, Rodriguez also plugged in a "SanDisk" external storage device (serial number: 4C530000280605123272) and transferred other commercially sensitive information. In all, these files included a treasure trove of information about Plaintiffs' pricing, bidding strategy, project management and completion strategies, designs, budgets, cost information and summaries, payroll,

[7] To protect the commercially sensitive nature of this project, Plaintiffs have renamed it "Sensitive Project No. 3."

privileged legal advice, risk analyses, confidential financial statements (of Plaintiffs and third parties which are protected by confidentiality agreements with those third parties), confidential agreements, and executive presentations. (FAC ¶ 63). Examples of this critical information includes the following files related to bids where Acciona will compete against Ferrovial's construction division:

- Sensitive Project No. 1:
  - "[Sensitive Project No. 1] Longitudinal Study Meeting notes 20241001."
  - "2024.09.03_[Sensitive Project No. 1]_Stick_Diagram_v6 1.xlsx."
  - "Alternatives for [Sensitive Project No. 1].pptx."
- Sensitive Project No. 2:
  - "Cintra [Sensitive Project No. 2] Cost Scenarios.docx."
  - "[Sensitive Project No. 2] Strategic Plan v1.pdf."
  - "Due Diligence-[Sensitive Project No. 2]."
- Sensitive Project No. 3:
  - "Estimate [Sensitive Project No. 3]_Revision-May 6 2024.xlsx."
  - "Sensitive Project No. 3] I-5718.pdf."
  - "Estimate [Sensitive Project No. 3] (Analysis of [Sensitive Project No. 3[V_3.xlsx."
  - "Conceptual Unsolicited Proposal – [Sensitive Project No. 3] (Shared Version).pdf."

(FAC ¶ 63).

24. Additionally, Rodriguez took essential documents related to the SR400 Express Lanes Project and East Interchange Project, which will aid in the ongoing bids. These projects are situated near one of the Sensitive Projects and contain vital information on risk allocation, as well as cost details related to pricing, fees, overhead, and escalation. (FAC ¶ 64). Then, throughout October, Rodriguez also plugged in another external storage device bearing serial number 6370801026293018812. (FAC ¶ 65).

25. However, Rodriguez's employment ended on or about November 20, 2024, and Rodriguez did not return those external storage devices that contained Plaintiffs' information. And Rodriguez neither informed Plaintiffs that he had transferred the commercially sensitive data to the external storage devices nor requested permission to keep the data that he had transferred. Instead, Rodriguez took those external storage devices with him and remained in possession of them as his employment with Acciona commenced. (FAC ¶ 66).

26. As with Gonzales, the only reason that Rodriguez would have transferred the data to those external storage devices shortly before his employment ended was to have and be able to use the data during his new employment with Acciona. (FAC ¶ 67). In fact, on April 4, 2025, Rodriguez indicated that he plugged in the "My Passport" into his Acciona computer, thereby exposing Plaintiffs' commercially sensitive data to Acciona, a direct competitor. (FAC ¶ 68).

Human Resources Manager Valdes

27. Plaintiffs' investigation also confirmed that Valdes was at least equally culpable. Like Gonzalez and Rodriguez, Valdes was a long-time, trusted employee of the Ferrovial family of companies. Before leaving and joining Acciona, Valdes was employed as a Human Resources Manager, with access to sensitive information relating to staffing plans, various trainings, and wage data. On October 21, 2024, Valdes plugged a "Toshina External USB" (serial number: F90741050010202) into his work computer and transferred numerous of these types of documents from Plaintiffs' computing network. Then, on November 11, 2024, Valdes plugged in a second external storage device — a "Western Digital Elements 2621" (serial number: WXU2E514URR) — and transferred more of these types of documents, including a highly sensitive file titled "Grand Employee Lists."[8] (FAC ¶ 69).

28. These documents are not insignificant, as the following examples of stolen information show:

- The "Grand Employee Lists" file is a master employee roster which contains personal confidential information on an employee (including social security numbers, dates of birth, ethnicity, salaries and home addresses), and accessing this data is an essential function of day-to-day HR work that is never allowed to be removed from Ferrovial's computing network.

[8] Additionally, the forensics show that, on August 21, 2024, Valdes also plugged in a "Samsung Flash Drive" (serial number 0372221040010034) into his work computer. That drive has not be return or accounted for.

- Trainings and policies that are used to increase the competence and knowledge base of Plaintiffs' employees;
- Various PE License, exam information, certifications, and similar information that can improve employees' candidacy for future development; and
- Employee resumes and information that highlights knowledge, skill and experience of a candidate that are often used for succession and talent plans, as well as illustrate competence to Plaintiffs' clients for key roles.

(FAC ¶ 70). In fact, Acciona has already benefitted from the retention of this information, as numerous employees of Plaintiffs have been solicited and convinced to end their employment with Plaintiffs and join Acciona, including at least five individuals who are not presently named as defendants in this civil action (that is, in total, Acciona has successfully targeted and convinced at least twelve individuals to join its ranks in just a short time). (FAC ¶ 71).

29. Not only did Valdes never have — nor seek — permission to remove and use Plaintiffs' sensitive data, but even when confronted with evidence of this misconduct, Valdes continued to hide the fact that he had used this second external storage device. Through communications with counsel, Valdes insisted that there was only one device that he had used and retained (the "Toshiba External USB"). But on April 3, 2025, Valdes finally admitted that he had, in fact, retained the "Western Digital Elements 2621" drive. Notably, this admission only came after being confronted with contrary forensic evidence; and, even then, Valdes tried to excuse his obfuscation by claiming that he had a faulty memory and that his wife

had placed the "Western Digital Elements 2621" drive in a drawer without him knowing. (FAC ¶ 72).

Investigative Stage Three: Beltran and Bregel

30. Beltran and Bregel were no better. Plaintiffs' continuing investigation revealed that, between them, they also misappropriated hundreds of thousands of files using external storage devices. And, not unlike the others, Beltran and Bregel had been employed with Ferrovial for more than two decades, having most recently worked for ANC as Vice-President of Construction and Cost Controls Manager, respectively. (FAC ¶ 73).

31. For instance, on February 3, 2025 — some fifteen days before her actual departure, but only a day or so before submitting notice of her resignation — Bregel plugged in a JMicron external storage device and began transferring a significant amount of work-related emails that included information and attachments relating to subcontractors' monthly closures, project budgets, and employee wage information. She also transferred project layouts and designs. (FAC ¶ 74). She continued this activity on February 14, 2025, again by using the JMicron external storage device; this time transferring the contract for a large-scale project. And then on February 16, 2025, she also transferred a number of documents to the JMicron device, including further cost-related documents, procurement contracts, and various design files. (FAC ¶ 75).

32. Her expropriation of Plaintiffs' data continued, when, on February 18, 2025, she went on to transfer more monthly closings, various contracts, procurement breakdown spreadsheets, procurement plans, supplier information, office budgets, comparative pricing spreadsheets, risk assessments, pricing quotes and estimates, and business opportunity matrices. And on February 19, 2025, Bregel plugged in another external storage device (a UDisk) and compounded her theft of company information by downloading payroll data. (FAC ¶ 76).

33. To make matters worse, Bregel's husband — Beltran — also used that JMicron from February 13-18, 2025, to transfer what appears to be hundreds of thousands of documents. This includes ANC's Construction and Design Contact List for the project, ANC videos, various purchase contracts, design and drawing files, project-related files (including plans, contracts, schedules, monthly cost data, accruals, and proposal data), technical submissions, subcontractor quotes, and tender phase documents. (FAC ¶ 77). In fact, it appears that Beltran used that same JMicron external storage device to transfer every – or practically every – quote and proposal ANC received from potential vendors and subcontractors during the bid phase of its project, each of which contains sensitive pricing (and other competitive) information. (FAC ¶ 78).

34. Bregel and Beltran — like Gonzalez, Rodriguez, and Valdes — did not inform anyone at ANC that they transferred this trove of highly sensitive data to

their external storage devices. And they certainly did not return them when they resigned. Instead, they ensured that they would retain possession of those devices (and their voluminous contents) in their new roles at Acciona as "Executive Construction Director" and "Construction Manager Bid Phase," respectively. (FAC ¶ 79).

35. Bregel and Beltran have also significantly delayed returning the misappropriated information. (FAC ¶ 80). On February 21, 2025, undersigned counsel sent a letter to Bregel and Beltran, alerting them to the suspicious computing activity that was recently discovered and demanding, among other things, the return of devices that contained misappropriated information and access to accounts that may also contain such information. Four days later, on February 25, 2025, undersigned counsel received a letter in response, stating that Bregel and Beltran were being represented by counsel. (FAC ¶ 81). However, it was not until April 8, 2025, that Bregel and Beltran's counsel provided a substantive response, despite multiple requests for one. But even then, while Bregel and Beltran confirmed that they were in possession of an external hard drive, two other external storage devices, two cellphones, and one iPad, they did not provide a date certain for the return of those devices. (FAC ¶ 82).

Defendants Misappropriated Ferrovial's Playbook and are Competing Unfairly

36. Since filing the original lawsuit, Plaintiffs have attempted to resolve this dispute and hoped that these individuals, as well as Acciona, would be reasonable, admit their wronging doing, and accept some measures to ensure fair competition. (FAC ¶ 83). Plaintiffs have been disappointed on all counts, which has necessitated the filing of this First Amended Complaint. (FAC ¶ 84).

37. On April 4, 2025, Plaintiffs learned through their own efforts that at least one of the external storage devices was likely connected to Acciona's computing network. And, despite their sincere hopes of resolving things amicably, Plaintiffs continuing to encounter little more than obstruction and obfuscation from Defendants. (FAC ¶ 85).

38. For its part, Acciona was slow to respond to Plaintiffs' concerns that were first raised on February 27, 2025. For instance, Plaintiffs received a response from Acciona's outside counsel at Jones Day about a week later (on March 7, 2025), notifying Plaintiffs that Jones Day had been retained and would be providing a substantive response on Acciona's behalf the following week. No response was received and on March 14, 2025, undersigned counsel followed up regarding a status of the response, at which time Acciona responded stating only that it was still looking into Plaintiffs' concerns and would have a substantive response within two weeks. No response was received and on March 27, 2025 undersigned counsel again

followed-up and on March 28, 2025 Acciona stated the response would be forthcoming the following week. Finally, on April 7, 2025 — over a month from Plaintiffs' initial February 27 letter — Acciona finally responded substantively, but offered no solution to locate and return Ferrovial's stolen information. (FAC ¶ 86).

39. Though there were several self-serving and vague statements, Acciona confirmed important details, including that Rodriguez — who plugged an external storage device filled with Plaintiffs' commercially sensitive data into his Acciona-issued computer — is managing the implementation phase of Acciona projects across the entire United States. Further, Acciona does not deny that documents were moved to or accessed from Acciona's computing network and, in fact, Acciona stunningly concedes that documents were indeed moved to Acciona's computing network. (FAC ¶ 87).

40. While Acciona's eventual response to Plaintiffs' concerns raises any number of issues, one thing is certainly clear. Stopping the harm flowing from, and threatened by, Defendants' misappropriation of Plaintiffs' data is of paramount importance because the documents exfiltrated comprise some of Plaintiffs' most critical business information. (FAC ¶ 88).

41. For instance, Gonzalez misappropriated engineering designs and stick diagrams relating to projects that comprise strategies for maximizing revenue on projects; internal communications comprising unique strategies for bidding these

large-scale infrastructure projects; design quality management plans that contain Plaintiffs' proprietary design processes to establish overall design production, review, and implementation process that impact pricing in numerous ways; various due diligence documents that reflect Plaintiffs' bidding approach that reveals their unique approach to bidding on projects; pricing documents that reflect a unique approach and strategy for bidding on large-scale projects; risk summaries and registers that set forth projected costs and contingencies and include forecasted opportunities for design optimization not fully fleshed out in the bid design, all of which reflect company principles that enhance Plaintiffs' competitive advantage; draft agreements and strategy comments contained therein; various pricing documents; and technical proposals. (FAC ¶ 89). Rodriguez has misappropriated these same types of documents — but for far more projects — and Valdes has misappropriated highly sensitive workforce related data. Similarly, the husband-and-wife team of Beltran and Bregel also misappropriated these same types of documents relating to other projects. (FAC ¶ 90).

42. Taken together, the misappropriated information essentially provides a competitor — like Acciona — with the blueprints to strip or severely minimize Plaintiffs' competitive advantage. In the hands of a direct competitor, like Acciona, this information is devastating to Plaintiffs. (FAC ¶ 91). This is especially true considering that Gonzalez misappropriated information relating to projects that are

not only still out for bid but also are being competitively bid on by his new employer, Acciona. In other words, through the Individual Defendants' surreptitious, unauthorized transfer and retention of this information and their current employment, Acciona effectively has access to the misappropriated information. (FAC ¶ 92).

LAW AND ARGUMENT

I. Preliminary Injunction is both Warranted and Necessary.

43. To obtain a preliminary injunction, the moving party must establish four elements: "[i] A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, [ii] that he is likely to suffer irreparable harm in the absence of preliminary relief, [iii] that the balance of equities tips in his favor, and [iv] that an injunction is in the public interest." *Winter v. NRDC, Inc.*, 555 U.S. 7, 20 (2008); *LSSI Data Corp. v. Comcast Phone, LLC*, 696 F.3d 1114, 1119 (11th Cir. 2012); Fed. R. Civ. P. 65.

44. Preliminary injunction is necessary in the present case to prevent Defendants from using, disclosing, and retaining misappropriated trade secrets (or, in some instances, continuing to do so). Only the requested injunctive relief will prevent Defendants from gaining and/or further exploiting an unjust and unlawful competitive advantage. And, in support of their request, Plaintiffs would show this Court — as set forth below — that they satisfy each of the four required elements.

First, the evidence demonstrates that Plaintiffs are likely to succeed on the merits of their trade secret claims against the Defendants — Plaintiffs took reasonable steps to protect the confidentiality of its information, and the information has economic value because it is confidential. Further, forensic evidence demonstrates that Plaintiffs misappropriated this information shortly before they resigned and in preparation for joining Acciona. *Second*, Plaintiffs are suffering and will continue to suffer irreparable harm due to the nature of the misappropriated trade secret information being in possession of and accessible by a competitor. *Third*, the balance of the equities weighs in favor of Plaintiffs. And *fourth*, granting the requested relief best serves the public interest by promoting fair competition and business practices.

A. Plaintiffs are likely to succeed on the merits of its trade secret claims.

45. Likelihood of success of the merits is "generally the most important" of the four preliminary injunction factors, and it "requires a showing of only *likely* or probable, rather than *certain*, success." *Schiavo ex rel. Schindler v. Schiavo*, 403 F.3d 1223, 1232 (11th Cir. 2005) (emphasis in original). Plaintiffs can satisfy this burden for their claims because the evidence overwhelmingly shows that Defendants misappropriated their trade secrets.[9]

[9] The DTSA, GTSA, and TUTSA have similar definitions. For efficiency sake, Plaintiffs explain why they will likely prevail on its claims under the DTSA against the Defendants and the

46. The DTSA states that an "owner of a trade secret that is misappropriated may bring a civil action" in federal court "if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b). The DTSA defines "misappropriation" as "(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (B) disclosure or use of a trade secret of another without express or implied consent by a person who," among other things, "used improper means to acquire knowledge of the trade secret." 18 U.S.C. § 1839(5)(A)-(B). Under the DTSA, prohibited "misappropriation" includes the acquisition of a trade secret by improper means, as well as its use or disclosure. *See id.* at § 1839(5)(A)-(B). The DTSA defines "improper means" as including "theft bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." *Id.* at § 1839(6)(A). The DTSA, moreover, defines a "trade secret" as:

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if — (A) the

GTSA against Gonzalez, Rodriguez, Valdes, and Acciona, but for those same reasons, it will also likely prevail on its trade secret claims under the TUTSA against Beltran, Bregel, and Acciona.

> owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily available through proper means by, another person who can obtain economic value from the disclosure or use of the information.

18 U.S.C. §1839(3).

47. Evidence demonstrates that the Individual Defendants' actions shortly before leaving the Ferrovial family of businesses qualify as a "misappropriation" that was achieved through "improper means." Specifically, with knowledge that Plaintiffs' information was confidential and not to be disseminated other than for Plaintiffs' benefit, the Individual Defendants transferred this information, without authorization and in violation of Plaintiffs' policies, to external hard drives for Acciona's use. *See Sci. Games Int'l, Inc. v. Cash*, No. 16- 142, 2017 U.S. Dist. LEXIS 233341, at *13-15 (N.D. Ga. Jan. 25, 2017) (holding that a plaintiff showed a likelihood of success on the merits for its misappropriation claim based on the defendant's past downloading activities); *Westrock v. Larry Health Sealy*, No. 2:20-cv-00180-RWS, 2021 U.S. Dist. LEXIS 121769, at *10-11 (N.D. Ga. Mar. 23, 2021) (holding that under both the DTSA and its Georgia counterpart, an employer successfully showed that they could plausibly prove misappropriation by providing evidence that their former employee downloaded thousands of documents before and after receiving an offer of employment from a competing company and

connected their external hard drive to their company computer after beginning work for the competitor). Further, Defendants now have this information to compete unfairly against Plaintiffs.

48. The misappropriated information, moreover, qualifies as trade secrets. The files identified through the computer forensics contain highly sensitive business information that is not generally known and gives Plaintiffs a competitive edge. Further, Plaintiffs took reasonable efforts to maintain the secrecy of this information by requiring its employees — including the Individual Defendants — to agree to abide by policies protecting the confidentiality of the information; by limiting personnel's access to certain confidential business information; and by password-protecting that information. *See* Unif. Trade Secrets Act § 1(4)(ii) cmts. (drafters of Uniform Trade Secret Act, upon which the DTSA (as well as the GTSA and TUTSA) is based, explain that "reasonable efforts to maintain secrecy" may include advising employees of the existence of a trade secret or limiting access to a trade secret on a "need to know basis").

49. Plaintiffs' efforts to maintain the confidentiality of this information gives it "independent economic value." A direct competitor would benefit greatly if it had access to the information that the Individual Defendants misappropriated. With this type of information and the other misappropriated information, Acciona, for instance, is immediately put in an enhanced position to compete, with nearly

complete knowledge of how Plaintiffs go to market and compete for large-scale projects. Further, Defendants obtained all of this information unfairly and without having to invest the time, money, and resources that Plaintiffs expended over many years to develop the information.

50. In sum, Plaintiffs can establish that it will likely prevail on the merits of their trade secret claims because Defendants misappropriated, by improper means, Plaintiffs' information and data, which qualify as trade secrets.

B. Plaintiffs will suffer irreparable harm in the absence of a temporary restraining order.

51. Plaintiffs have suffered, and will continue to suffer, irreparable harm if the requested relief is not granted. Irreparable injury is harm that "cannot be undone through monetary remedies." *Northeastern Florida Chapter of Ass'n of General Contractors v. Jacksonville*, 896 F.2d 1283, 1285 (11th Cir. 1990); *Cunningham v. Adams*, 808 F.2d 815, 821 (11th Cir. 1987). Both the Eleventh Circuit, generally, and the Northern District of Georgia, specifically, recognize that irreparable harm can be established, even where injuries are difficult to quantify. *MacGinnitie v. Hobbs Group, LLC*, 420 F.3d 1234, 1242 (11th Cir. 2005); *J. Lee Gregory, Inc. v. Amcor Indus.*, No. C-78-703-A, 1978 U.S. Dist. LEXIS 14162 at *9 (N.D. Ga. Nov. 27, 1978) (stating, "[t]he difficulty of ascertaining accurate compensation in damages has been a long-standing basis for irreparable harm in Georgia."). Notably, in this regard, the DTSA recognizes not only that irreparable injury arises from the

misappropriation of trade secrets, but also makes clear that even the *threat* of misappropriation may be enjoined. 18 U.S.C. § 1836 (b)(3)(A)(i).

52. Here, Plaintiffs can show that the Individual Defendants improperly stole trade secrets and have continued to maintain their possession of trade secrets as employees of Acciona. It is similarly evident that those trade secrets, in the hands of a competitor, provide an unfair competitive advantage, which is sufficient to show a threat of irreparable harm. *See G.W. Henssler & Assocs., Ltd. V. Marietta Wealth Mgmt.*, No. 17-2188, 2017 U.S. Dist. LEXIS 220400, at *15-16 ("[l]oss of confidential and proprietary information is per se irreparable harm" under O.C.G.A. § 10-1-762(a));); *Cash*, 2017 U.S. Dist. LEXIS 233341, at *17-18 (finding possession of trade secret and being in a position to use that information sufficient to show irreparable harm); *Priority Payment Sys., LLC v. Signapay, LTD*, 161 F. Supp. 3d 1294, 1303 (N.D. Ga. 2016) (finding the use of trade secrets would injure the plaintiff's competitive market advantage); *Arclin United States v. Vits Tech. Gmbh*, 2020 U.S. Dist. LEXIS 256083, at *8 (N.D. Ga. Mar. 31, 2020) ("the loss of trade secrets is an irreparable harm"); *Specialty Chems. & Servs. V. Chandler*, No. 87-2338, 1988 U.S. Dist. LEXIS 16090 at *14 (N.D. Ga. Sept. 26, 1988) (stating that in light of evidence showing that defendants possess a number of Specialty's trade secrets, the threat of disclosure or use is significant); *Amedisys Holding, LLC v. Interim Healthcare of Atlanta*, 793 F. Supp. 2d 1302, 1314 (N.D. Ga. 2011)

(holding that under the GTSA, the employer suffered irreparable harm where the defendant made repeated misrepresentations about their downloading of trade secrets causing the Court to be unsure of whether the defendant still had the trade secrets in their possession).

53. Plaintiffs face the very real threat of actual irreparable harm if the Court does not enter a preliminary injunction. The Individual Defendants improperly stole and retained Plaintiffs' trade secrets on external storage devices and now Defendants are in a position to use those trade secrets for their illicit benefit and to Plaintiffs' detriment. With Plaintiffs' trade secrets readily accessible, Acciona can unlawfully compete against and harm Plaintiffs — courtesy of the trade secret data unlawfully procured by their new employees, the Individual Defendants — resulting in injuries to Plaintiffs that will prove difficult to measure with monetary precision.

C. Plaintiffs' injury outweighs any harm to Defendants.

54. Next, the Court must determine whether the threatened injury to Plaintiffs outweighs any damage that an injunction might cause. *Winter*, 555 U.S. at 24 ("in each case, courts must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of requested relief) (citations omitted); *Ivc Us v. Hauli Group United States*, No. 21-042, 2021 U.S. Dist. LEXIS 119098, at *13 (N.D. Ga. Apr. 2, 2021). Plaintiffs seek narrowly tailored relief designed to protect their legitimate business interests and to ensure that

misappropriated information cannot be used further to unfairly compete. Without this Court's intervention, Plaintiffs stand to lose the value of their intellectual property to Defendants. In contrast, however, Defendants will suffer no undue hardship because of the requested injunctive relief, as this relief would merely require Defendants to comply with existing trade secret law. *See Westrock Servs., LLC v. Roberts*, No. 1:22-CV-01501-SCJ, 2022 U.S. Dist. LEXIS 96235 at *16-17 (N.D. Ga. May 4, 2022) (finding that granting an injunction where the defendant's misappropriation violated their contractual obligations does not legally harm the defendant because it "merely maintain[s] the status quo"); *G.W. Henssler & Assocs., Ltd. v. Marietta Wealth Mgmt,, LLC*, No. 1:17-cv-2188, 2017 U.S. Dist. LEXIS 220400, at *16 (N.D. Ga. Oct. 23, 2017) (finding in a misappropriation case that "[i]t is both equitable and in the public interests to require Defendants to abide by the law."); *Amedisys Holding, LLC v. Interim Healthcare of Atlanta, Inc.*, 793 F. Supp. 2d 1302, 1314-1315 (N.D. Ga. 2011) ("Mack, on the other hand, 'cannot suffer compensable harm when enjoined from an unlawful activity'"); *Dish Network L.L.C. v. Ramirez*, No. 15-04712, 2016 WL 3092184, at *7 (N.D. Cal. Jun. 2, 2016) (balance of hardships tips in favor of plaintiff seeking an injunction when it would "do no more than require Defendant to comply with federal and state laws").

55. This Court should therefore find that the equities favor issuing the requested injunctive relief. Further, the requested forensic examinations will merely

allow the trade secrets and confidential business information that are unlawfully within Defendants' possession to be remediated permanently from their computing devices, network, and accounts.

D. Injunctive relief will not disserve the public interest.

56. Finally, enjoining Defendants from disclosing, using, and retaining possession of Plaintiffs' trade secrets will not disserve the public interest. Instead, the requested relief will promote fair competition, ethical behavior, honest work, and innovation. *G.W. Henssler & Assocs., Ltd.*, 2017 U.S. Dist. LEXIS 220400, at *16 (enjoining the use of stolen information and instructing that "[i]t is both equitable and in the public interest to require Defendants to abide by the law"); *Cash*, 2017 U.S. Dist. LEXIS 233341, at *18 (ruling that an injunction serves public interests under Georgia's "strong public policy in favor of protecting trade secrets" as the injunction "promote[s] fair competition"); *Amedisys Holding, LLC*, 793 F. Supp. 2d at 1314-1315 (finding that prohibiting the use of stolen information "will best serve the public interest" because "[t]here is a strong public policy promoting fair competition" and "[a]llowing Mack to compete unfairly and use Amedisys' trade secrets would undermine those policies."). Indeed, without a robust ability to protect trade secrets and other proprietary and confidential information, businesses will not be able to hire high-level employees or contractors and engage in fair and legitimate competition for fear of losing information to a competitor.

II. The Court Should Set a Preliminary Injunction Hearing and Grant Expedited Discovery Including a Forensic Examination of Defendants' Computing Devices and Networks.

57. An evidentiary hearing on Plaintiffs' request for preliminary injunction should be set. *See, All Care Nursing Serv., Inc. v. Bethesda Mem. Hosp., Inc*, 887 F.2d 1535, 1538 (11th Cir. 1989) (citation omitted) (stating that "where an injunction turns on the resolution of bitterly disputed facts . . . an evidentiary hearing is normally required to decide credibility issues."). During the evidentiary hearing, Plaintiffs will present evidence demonstrating why the Court should issue the requested preliminary injunction.[10] Further, as explained in detail in Plaintiffs' motion to expedite discovery, which is being filed concurrently with this motion, expedited discovery is appropriate to give the Court a more complete record to conduct a preliminary evaluation of the merits of Plaintiffs' claims and to allow it to ascertain the extent of Defendants' unlawful misappropriation.

58. This Court has entered the very relief Plaintiffs request in at least one similar trade secret case. *See Marietta Wealth Mgmt., LLC*, 20117 U.S. Dist. LEXIS 220400, *18 (entering preliminary injunction prohibiting use of information,

[10] Plaintiffs note that, in light of the indisputable and overwhelming forensic evidence of wrongdoing uncovered to date, the Court would be well within its discretion to grant the requested relief even without an evidentiary hearing. *See McDonald's Corp. v. Robertson*, 147 F.3d 1301, 1310-1314 (11th Cir. 1998) ("We therefore conclude that the district court did not err in denying Robertson's motion for evidentiary hearing and in granting McDonald's motion for preliminary injunction."). This is especially so if, in their responsive briefing, Defendants can do little to contest the facts set forth in Plaintiffs' verified pleading. *See id.*

requiring return of misappropriated information, and requiring defendants to "turn over business and personal hard drive(s) and computer(s) and to provide access to their cloud-based computer storage services (such as Dropsend.com and/or Dropbox.com), and their email accounts for a forensic examination") (emphasis added).

59. To maintain the *status quo* before Defendants' unlawful misappropriation of Plaintiffs' trade secrets, Plaintiffs should be allowed to commence expedited discovery, conducting a forensic analysis of the computing devices, networks, and accounts used and accessed by the Individual Defendants, including Acciona's computing devices, networks, and accounts to which the Individual Defendants had access, to determine the extent of the misappropriation and begin to remediate that stolen information.

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request the Court set an evidentiary hearing on Plaintiffs' request for a preliminary injunction, and thereafter enter the proposed preliminary injunction.

Respectfully submitted:

/s/ Joseph F. Lavigne

*Joseph F. Lavigne
*P.J. Kee
JONES WALKER LLP
201 St. Charles Avenue – 50th Floor

New Orleans, Louisiana 70170-5100
Telephone: 504-582-8000
Email: jlavigne@joneswalker.com
Email: pkee@joneswalker.com
Jones Walker, LLP

and

Chad v. Theriot
JONES WALKER LLP
3455 Peachtree Road NE, Suite 1400
Atlanta, GA 30326
Telephone: 404-870-7515
Email: ctheriot@joneswalker.cm

Counsel for Plaintiffs Ferrovial Construction US Corp. and North Perimeter Contractors, LLC
*****Admitted Pro Hac

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was served on Defendants, including newly added Parties, through their counsel by email on April 21, 2025.

/s/ Joseph F. Lavigne
*Joseph F. Lavigne